ABSTRACT

An approximate message authentication code (AMAC) which, like conventional message authentication codes, provides absolute authentication of the origin of the message, yet provides an approximate integrity check for the content of the message. The approximate integrity check will be computed probabilistically and will likely be the same for messages having only a small percentage of different bits. A distance measure on the AMACs, such as a Hamming distance measure, may be used to determine whether the number of bit differences between the messages is likely to be within an acceptable amount. The AMAC is a probabilistic checksum based on a shared key. The AMAC uses the message and a shared key as inputs. Optionally, an initial value may also be used as an input. In one version of the invention, the data in the message M are permuted and arranged (physically or logically) into a table having $|A|$ bits in each column and T^2 rows, where T is may be an odd integer. The permuted data are masked, for example, to generate an unbiased, independent, identically distributed set of bits (1s and 0s). Taking T rows at a time, the majority bit value for each column is determined and that majority value is used to generate a new row. This procedure is repeated on the T new rows of majority bits. The resulting $|A|$bits is the AMAC.